Technical Bulletin: Cisco Talos CVEs

Date of issue: 30 Apr 2019

Applicable Products

This technical bulletin applies to the following Airlink products:

- LS300, GX400, GX440 and ES440 running ALEOS 4.4.8 or earlier
- GX450 and ES450 running ALEOS prior to version 4.9.4
- MP70, MP70E, RV50, RV50X, LX40 and LX60 running ALEOS prior to version 4.12

Summary

Researchers from Cisco Talos have reported several possible vulnerabilities in ALEOS, the embedded software that runs on Sierra Wireless AirLink gateways and routers. All the reported vulnerabilities require authenticated access to the gateway via use of a valid username and password, or for an authorized user to click on a malicious link while also logged into the gateway. Several of the reported vulnerabilities are not applicable as they describe normal and intended operation of the gateway. The remainder of the vulnerabilities have been addressed in the latest versions of ALEOS for the affected products or, in select cases, by using modern web browsers, such as Chrome, Firefox or Edge, with in-built cross-site scripting (CSS) and cross-site-request forgery (CSRF) protection.

Sierra Wireless has worked closely with Talos to understand the details of the reported vulnerabilities. The following table summarizes the score for each vulnerability calculated using the information received and the CVSSv3 calculator.

CVE ID	Title	Sierra Wireless CVSSv3 Score
CVE-2018-4061	ACEmanager iplogging.cgi command injection vulnerability	**9.1** (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
CVE-2018-4062	SNMPD hard-coded credentials vulnerability	**6.2** (AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:H)
CVE-2018-4063	ACEmanager upload.cgi remote code execution vulnerability	**9.1** (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
CVE-2018-4064	ACEmanager upload.cgi unverified password change vulnerability	**Not applicable -** The original password must first be used to authenticate as "user" before the "user" password can be changed via ACEmanager_upload.cgi

CVE-2018-4065	ACEmanager ping_result.cgi cross-site scripting (CSS) vulnerability	**6.1** (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2018-4066	ACEmanager cross-site request forgery (CSRF) vulnerability	**6.8** (AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H)
CVE-2018-4067	ACEmanager template_load.cgi information disclosure vulnerability	**4.1** (AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N)
CVE-2018-4068	ACEmanager information disclosure vulnerability	**Not applicable -** No sensitive information is disclosed – details on gateway default configuration are provided in publicly available user guides
CVE-2018-4069	ACEmanager information exposure vulnerability	**5.9** (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVE-2018-4070, CVE-2018-4071	ACEmanager Embedded_Ace_Get_Task.cgi information disclosure vulnerability	**Not applicable –** The administrative user ("user") and local software processes running on the gateway are explicitly authorized to access configuration and status information in order to perform normal gateway operations.
CVE-2018-4072, CVE-2018-4073	ACEmanager Embedded_Ace_Set_Task.cgi permission assignment vulnerability	**Not applicable** - The ability for the administrative user ("user") and local software processes running on the gateway to modify configuration values is intentional and necessary for normal gateway operation.

The following table shows the software versions that resolve the applicable vulnerabilities for each affected product.

	Products		
CVE ID	**LS300, GX400, GX440 and ES440**	**GX450 and ES450**	**MP70, MP70E, RV50, RV50X, LX40 and LX60**
CVE-2018-4061	ALEOS 4.4.9	ALEOS 4.9.4	ALEOS 4.11
CVE-2018-4062	ALEOS 4.4.9	ALEOS 4.9.4	ALEOS 4.12
CVE-2018-4063	ALEOS 4.4.9	ALEOS 4.9.4	ALEOS 4.11
CVE-2018-4065	(1)	ALEOS 4.9.4	ALEOS 4.11
CVE-2018-4066	(1)	(1)	ALEOS 4.11
CVE-2018-4067	ALEOS 4.4.9	ALEOS 4.9.4	ALEOS 4.11
CVE-2018-4069	This vulnerability can be mitigated by configuring the gateway to use HTTPS only for ACEmanager access (see Recommended Actions section)		

(1) These vulnerabilities can be mitigated by using a modern browser with CSS and CSRF protection, such as Chrome, Firefox and Edge.

Recommended Actions

Sierra Wireless advises users to follow the recommended actions outlined below. If you require assistance performing these actions, please contact your authorized AirLink reseller or your Sierra Wireless sales or technical representative. Alternatively, you can also contact Sierra Wireless technical support for assistance:

1. Ensure a strong password is set for the 'user' account. For guidance on password strength, Sierra Wireless recommends the "memorized secret authenticator" guidelines in NIST SP800-63B. The user password can be set by navigating to *Admin* > *Change Password* in ACEmanager, AirLink Management Service (ALMS) or AirLink Manager (AM).
2. If ALEOS Application Framework (AAF) is enabled, ensure a strong password is set for the AAF User account. The AAF User password can be set on the *Admin* > *Change Password* page.
3. If Telnet or SSH is enabled, ensure a strong password is set for the sconsole account. The sconsole password can be set on the *Admin* > *Change Password* page.
4. When connecting directly to ACEmanager:
    a. Use HTTPS. The gateway can be configured to only accept HTTPS connections by setting *Services* > *ACEmanager* > *Local Access* and *Services* > *ACEmanager* > *Remote Access* to HTTPS only. These configuration changes can be made using ACEmanager, ALMS or AM.
    b. Utilize an up-to-date, modern web-browser with built-in CSS and CSRF protection, such as Chrome, Firefox or Edge.
5. Upgrade to the latest version of ALEOS for your product(s), when available:
    a. LS300, GX400, GX440 and ES440: **ALEOS 4.4.9**
    b. GX450 and ES450: **ALEOS 4.9.4.p09** (available now)
    c. MP70, MP70E, RV50, RV50X, LX40 and LX60: **ALEOS 4.12**

Support Contact Information

Sierra Wireless Technical Support is available by phone or web portal from 6:00 to 17:00 PST, Monday to Friday.

Phone (Toll Free): 1-877-687-7795

Web: https://www.sierrawireless.com/support/community-portal/